REMARKS

Claims 1-47 are pending. Claims 1-47 stand rejected.

Reconsideration is requested. The rejections are traversed. No new matter is added. Claims 1-47 remain in the case for consideration.

While the Examiner rejects claims 1-47 in the Office Action dated September 21, 2006, the Examiner has not provided a specific reason as to why any of the claims have been rejected. Presumably, claims 1-46 stand rejected for the reasons stated in the Office Action dated June 9, 2006: specifically, the Applicant treats claims 1-46 as standing rejected under 35 U.S.C. § 103(a) as being unpatentable over Windows 2000 Authentication (http://www.comptechdoc.org/os/windows/win2k/win2kauthentication.html) ("Comptech Article").

The Applicant would like to point out that claim 47 was added in the response to the Office Action dated June 9, 2006, and therefore has never before been specifically rejected. The Applicant treats claim 47 as rejected under 35 U.S.C. § 103(a) as being unpatentable over "Comptech Article", but would appreciate the Examiner explaining why claim 47 should be rejected.

At this point, there are three issues in this patent application. These issues are:

- Can, will, and must the Applicant submit the affidavit requested by the Examiner?
- Can the Examiner rely on an Internet publication ("Comptech Article") dated after the Applicant's filing date in rejecting the pending claims, where there is no evidence that the teachings attributed to "Comptech Article" were, in fact, publicly known prior to the publication date of "Comptech Article"?
- Assuming arguendo that "Comptech Article" is proper prior art, are the pending claims rendered obvious by "Comptech Article"?

These three issues are discussed in turn below.

- Can, will, and must the Applicant submit the affidavit requested by the Examiner?

The Applicant cannot submit the requested affidavit

The Examiner states that "Applicant has explained and answered all issued presented by the Office except that of the affidavit. . . . Applicant is respectfully requested to either explicitly refuse to provide such an affidavit or to provide such an affidavit. . . . The Office notes that the affidavit would render moot all other issues. Thus, for the sake of compact prosecution, the Office awaits Applicant's answer regarding the affidavit before issuing another Office Action from the Examiner" (*see* Office Action dated September 21, 2006, page 2; emphasis in original).

The Applicant appreciates the Examiner's offer of an additional response to submit the indicated affidavit, and that the Examiner did not make the Office Action dated September 21, 2006 final. But the Applicant did not include the indicated affidavit with the response to the Office Action dated June 9, 2006 because the Applicant could not make such an affidavit. The Applicant therefore has to explicitly refuse to provide the indicated affidavit.

While the facts the Examiner wants recited in the indicated affidavit might be true, the Applicant cannot state that these facts are known by the Applicant to be true. The argument presented by the Applicant, for which the Examiner requests an affidavit, merely pointed out that the Examiner has failed to establish that the features described in "Comptech Article" were part of Microsoft Windows 2000 as of its original release. The Applicant was not stating that these facts were known to be true; the Applicant was only pointing out that the Applicant believed the Examiner's argument was incomplete for failing to show that the features were part of the original release of Microsoft Windows 2000. The Applicant does not, in fact, know whether or not the features described in "Comptech Article" were included in the original release of Microsoft Windows 2000.

The Examiner is attempting to shift the burden to the Applicant

In the Office Action dated June 9, 2006, the Examiner states that "Applicant has asserted that the features of [Microsoft] Windows 2000 may not have been actually known to others as an actual feature until after the first release. This may be persuasive. Applicant is requested to file an appropriate affidavit stating that this is true" (*see* Office Action dated June 9, 2006, pages 2-3). But there is no legal requirement for such an affidavit.

In requesting the affidavit, the Examiner is attempting to shift the burden of producing evidence away from the Examiner to the Applicant. According to M.P.E.P. § 2142, "The legal concept of *prima facie* obviousness is a procedural tool of examination which applies broadly to all arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process. . . . The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness" (citations omitted).

That the burden lies on the Examiner is further shown in 35 U.S.C. § 102, which states that "[a] person shall be entitled to a patent unless" the Examiner can show the Applicant is not entitled to the patent). In other words, unless the Examiner can present a *prima facie* argument as to why the Applicant should be denied a patent, the Applicant is entitled to the patent. The Applicant has made sufficient arguments as to why "Comptech Article" is insufficient to rejecting the pending claims. The burden is now back on the Examiner to show why the rejection can be maintained, if the Examiner wants to maintain the rejection.

The request for an affidavit from the Applicant that the features of the claimed invention were not known before the Applicant's filing date is a request by the Examiner for the Applicant to prove that the features of the claimed invention were not known before the Applicant's filing date. As the initial burden under 35 U.S.C. § 103(a) is on the Examiner to show that the claimed invention was obvious, this attempt to shift the burden of producing evidence from the Examiner to the Applicant is inappropriate.

The Examiner is requesting the Applicant to prove a negative

To say that the Applicant needs to show that the features in dispute in this case were not publicly known before the filing date of the patent application is to require the Applicant to disprove the reference's applicability. In addition to attempting to shift the burden of producing evidence to the Applicant, as argued above, this burden-shifting would require an Applicant to prove a negative, which is generally impossible to do. The Applicant cannot prove that the features discussed in "Comptech Article" were not publicly known before the Applicant's filing date, and therefore cannot provide the requested affidavit.

As discussed above, the Examiner bears the burden of searching for what Microsoft Windows 2000 included in its original release: the Applicant does not bear this burden. Nevertheless, the Applicant's undersigned patent attorney conducted an investigation of the Microsoft website in an attempt to determine how Microsoft Windows 2000 performed authentication in its original release. The undersigned did not find any publications that would qualify as prior art, either that support the Examiner's contention that the original release of Microsoft Windows 2000 included the features described in "Comptech Article", or that the claimed invention was not known before the filing date of the patent application.

Thus, for the reasons stated above, the Applicant expressly declines to provide the requested affidavit.

- Can the Examiner rely on an Internet publication ("Comptech Article") dated after the Applicant's filing date in rejecting the pending claims, where there is no evidence that the teachings attributed to "Comptech Article" were, in fact, publicly known prior to the publication date of "Comptech Article"?

"Comptech Article" is not proper prior art under 35 U.S.C. § 103(a)

The Applicant has previously argued that "Comptech Article" is not proper prior art. According to the Office Action dated June 9, 2006, the Applicant's argument that "Comptech Article" cannot be considered valid prior art "is not persuasive because the Office cited the prior art as a teaching regarding the Microsoft Windows 2000 rather than the prior art being published in the year 2000" (*see* Office Action dated June 9, 2006, page 2).

This rationale expressly ignores both the M.P.E.P. and the statute, and should be reconsidered. Simply titling a 2001 article "Windows 2000 Authentication" does not make the reference prior art to a patent application filed in 2001.

As the Examiner is rejecting the claimed invention over "Comptech Article" under 35 U.S.C. § 103(a), the text of the statute is worth reviewing. According to 35 U.S.C. § 103(a):

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

Thus, for a reference to be available under 35 U.S.C. § 103(a), the reference must first qualify as prior art under 35 U.S.C. § 102. This point is explicitly repeated in M.P.E.P. § 2141.01, which states that "'[b]efore answering *Graham's* "content" inquiry [the analysis under 35 U.S.C. § 103(a) set out by the Supreme Court in *Graham v. John Deere*, 383 U.S. 1, 148 U.S.P.Q. 459 (1966)], it must be known whether a patent or publication is in the prior art under 35 U.S.C. § 102'" (quoting *Panduit Corp. v. Dennison Mfg. Co.,* 810 F.2d 1561, 1568, 1 U.S.P.Q.2d 1593, 1597 (Fed. Cir.), *cert. denied*, 481 U.S. 1052 (1987)). Therefore, before the Examiner can analyze a reference under 35 U.S.C. § 103(a), the Examiner must verify that the reference is prior art under some section of 35 U.S.C. § 102.

35 U.S.C. § 102 lists seven reasons why an Applicant might be denied a patent:

> A person shall be entitled to a patent unless -
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, or
> (c) he has abandoned the invention, or
> (d) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing of the application in the United States, or
> (e) the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language; or
> (f) he did not himself invent the subject matter sought to be patented, or
> (g)(1) during the course of an interference conducted under section 135 or section 291, another inventor involved therein establishes, to the extent permitted in section 104, that before such person's invention thereof the invention was made by such other inventor and not abandoned, suppressed, or concealed, or (2) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also

the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

It is worth noting that 35 U.S.C. § 102 states that "[a] person shall be entitled to a patent unless" some subsection of 35 U.S.C. § 102 is satisfied. In other words, the presumption is that the Applicant is entitled to a patent, unless there is a reason to deny the patent application.

Of the seven subsections in 35 U.S.C. § 102, subsections (c), (d), and (f) relate to actions of the Applicant. As the Applicant has not done anything to justify denying the Applicant this patent, these subsections do not apply. Subsection (e) pertains to issued patents and published patent applications, and subsection (g) deals with interferences and conflicts between multiple patent applications to the same subject matter. As "Comptech Article" is not another patent application, a published patent application, or an issued patent, subsections (e) and (g) do not apply. This leaves only subsections (a) and (b).

Both subsections (a) and (b) use dates to determine whether a reference can be used to reject a claim. Subsection (a) requires that the invention be "described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent": in other words, the date the reference was published must be at least before the filing date of the patent application. Subsection (b) requires that the invention be "described in a printed publication in this or a foreign country . . . more than one year prior to the date of the application for patent in the United States".

As previously argued, the earliest publication date for "Comptech Article" that can be determined is October 28, 2001. This is several months after March 22, 2001, the filing date of the patent application. Accordingly, "Comptech Article" is not available as a reference under either 35 U.S.C. § 102(a) or (b). But if "Comptech Article" is not available as a reference under 35 U.S.C. § 102(a) and (b), and is not available under any of subsections (c)-(g), then "Comptech Article" is not available at all under 35 U.S.C. § 102, and so is not available under 35 U.S.C. § 103(a) to argue that the claimed invention is obvious.

It is worth noting that 35 U.S.C. § 102(a) and (b) do not depend on the content of a reference for purposes of deciding whether the reference is prior art. 35 U.S.C. § 102(a) and (b) only care about the publication date of the reference. Thus, the Examiner's dismissal of the Applicant's argument that "Comptech Article" was not published before the filing date of the patent application is inappropriate.

The Applicant requests that the Examiner explain in detail why the Examiner thinks "Comptech Article" – a document published after the filing date of the patent application – is available as a reference under 35 U.S.C. § 103(a). **Specifically, the Applicant requests that the Examiner identify under which subsection of 35 U.S.C. § 102 the Examiner thinks "Comptech Article" qualifies as prior art, as required by 35 U.S.C. § 103(a), and explain why "Comptech Article" qualifies as prior art under that subsection of 35 U.S.C. § 102.**

The Examiner has not responded to the Applicant's arguments about the statute and the M.P.E.P.

In response to the Office Action dated September 8, 2004, the Applicant argued why, under both the statute and the M.P.E.P., "Comptech Article" is not proper prior art. As the Examiner made no response to the argument that "Comptech Article" is not proper prior art under the M.P.E.P., the Examiner's Office Action is incomplete. For the Examiner's convenience, this argument is restated here.

"Comptech Article" is a non-patent document, which the Examiner retrieved from an on-line database. According to M.P.E.P. § 2128, "Prior art disclosures on the Internet or on an on-line database are considered to be publicly available as of the date the item was publicly posted. If the publication does not include a publication date (or retrieval date), it cannot be relied upon as prior art under 35 U.S.C. § 102(a) or (b), although it may be relied upon to provide evidence regarding the state of the art". "Comptech Article", however, does not include a publication date, and the Examiner has failed to establish the publication date of "Comptech Article". The closest the Examiner has come to establishing a date for "Comptech Article" is the date the Examiner printed "Comptech Article": August 31, 2004. This means that "Comptech Article" is not prior art under 35 U.S.C. § 102(a) or (b), and therefore is not available as a reference under 35 U.S.C. § 103(a).

In the Office Action dated April 21, 2005, the Examiner responded to this argument, and argued that the reference "clearly states the date (year 2000)". The Applicant respectfully disagrees. The reference describes the Microsoft Windows 2000 operating system, but this does not define a date of publication. "WINDOWS 2000" as used in the title of "Comptech Article" is merely the name or trademark of the product, and does not establish a date. The only date provided anywhere by the Examiner is the date on the bottom right-hand corner of the page,

which indicates the date the Examiner printed the document: August 31, 2004. If the Examiner wishes to establish that this document was published before that date, the Examiner needs to prove the publication date: an unsupported assertion that the document was published in the year 2000 is insufficient. According to M.P.E.P. 901.06, "[a]ll printed publications may be used as references, the date to be cited being the publication date". The mere fact that the document discusses an object that existed in the year 2000 does not establish the document as having been published in the year 2000; without showing publication prior to the filing date of the patent application, the reference has not been shown to have been publicly known before the filing date of the patent application.

The Applicant made a separate effort to establish a date for "Comptech Article". The best date (of any sort) that the Applicant was able to establish for "Comptech Article" is October 28, 2001. The undersigned visited the URL of the reference (http://www.comptechdoc.org/os/windows/win2k/win2kauthentication.html), and found a set of links on the left side of the website page, which were omitted from the printout provided by the Examiner. . . . Upon selecting the link titled "Introduction", the undersigned was taken to the URL for the introduction to the document which included the reference. This document is entitled "The CTDP Windows 2000 Tutorial Version 0.6.1 Oct 28, 2001" (http://www.comptechdoc.org/os/windows/win2k/index.html). It is worth noting on the left column of both website pages, item 64 is titled "Authentication" and is a hyperlink that brings the reader back to the website page of the reference. . . . Given that the version of the introduction to the reference cited by the Examiner is dated October 28, 2001, this is the earliest date that can be assigned to the reference. (It is worth noting that even this date cannot be fixed as a publication date; it is the date on which the entire tutorial was considered complete, but does not provide any definitive date as to when the tutorial was actually made available to the public.) As October 28, 2001 is more than seven months after the filing date of this patent application, even this date fails to establish the reference as prior art.

In the Office Action dated June 9, 2006, the Examiner stated that the Applicant's argument that "Comptech Article" is not valid prior art was "not persuasive because the Office cited the prior art as a teaching regarding the [Microsoft] Windows 2000 operating system rather than the prior art being published in the year 2000" (*see* Office Action dated June 9, 2006, page 2). The Examiner's argument ignores both the statute and the M.P.E.P., which both require that

prior art be *published* at least before the filing date of the patent application. The reason for this requirement is to ensure that if the patent is denied, it is because the claimed invention was known before the filing date of the patent application. The burden is on the Examiner to find a reference that was *published* before the filing date of the patent application that teaches the features of the invention; "Comptech Article" fails to meet this requirement.

The Applicant's argument here is not that Microsoft Windows 2000 did not publicly disclose the features recited in "Comptech Article" (although, as argued below, the Applicant believes the claimed invention is not obvious over the description in "Comptech Article"). The Applicant's argument is that the Examiner has failed to show that the information disclosed in "Comptech Article" was publicly known before the filing date of the Applicant's patent application.

If the Examiner's reasoning were to be believed, it would mean that anyone can assert, after the fact, that an invention was previously known. Such an assertion would then be sufficient to invalidate a patent application. The Applicant suggests that this is inappropriate: all such an assertion proves is that, after the filing date of a patent application, someone thought the claimed subject matter might have been known before the filing date of the patent application. For example, a person could write an article today, describing techniques that might have been used in constructing the pyramid at Giza. But without corroborating evidence, the article is merely surmise, and does not establish that the people constructing the pyramid at Giza actually knew any of those techniques at the time. Similarly, without corroborating evidence that the information disclosed in "Comptech Article" was publicly known before the filing date of Applicant's patent application, the Examiner's mere assertion that the claimed subject matter was previously known is insufficient.

If the Examiner believes that Microsoft Windows 2000 teaches the claimed invention, the Examiner should find a reference published before the filing date of the patent application that teaches the claimed subject matter. The Examiner has acknowledged that "no other prior art of record teaches the claimed subject matter" (*see* Office Action dated June 9, 2006, page 3). The Applicant finds it hard to believe that if Microsoft Windows 2000 taught the claimed subject matter, as the Examiner insists, that there is no reference published before the filing date of the patent application that teaches the claimed subject matter.

As discussed above, the Applicant's undersigned patent attorney has conducted a review of the Microsoft website to determine how Microsoft Windows 2000 performed authentication in its original release, even though the Applicant does not bear the burden of conducting such a search. The undersigned has found no reference published before the filing date of the patent application that describes Microsoft Windows 2000 as including the cited features of "Comptech Article".

"Comptech Article" is hearsay evidence

The Examiner is attempting to use "Comptech Article" for the truth of the matter asserted – namely, that Microsoft Windows 2000 included authentication as described, before the filing date of this patent application (*see* Office Action dated June 9, 2006, page 2 ("the Office cited the prior art as a teaching regarding the [Microsoft] Windows 2000 rather than the prior art being published in the year 2000")). This is hearsay. According to Federal Rules of Evidence (FRE) Rule 801(c), "'[h]earsay' is a statement, other than one made by the declarant . . . offered in evidence to prove the truth of the matter asserted". According to FRE 802, "[h]earsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress". FRE 803-807 provide a number of exceptions to FRE 802, but none of these exceptions are applicable here. As "Comptech Article" is hearsay evidence and no exception to the hearsay rule permits the entry of "Comptech Article" as evidence, it should not be admitted in considering the patentability of the claimed invention.

In particular, FRE 807 is not applicable. FRE 807, titled "Residual Exception", states:

> A statement not specifically covered by Rule 803 or 804 but having equivalent circumstantial guarantees of trustworthiness, is not excluded by the hearsay rule, if the court determines that (A) the statement is offered as evidence of a material fact; (B) the statement is more probative on the point for which it is offered than any other evidence which the proponent can procure through reasonable efforts; and (C) the general purposes of these rules and the interests of justice will best be served by admission of the statement into evidence. However, a statement may not be admitted under this exception unless the proponent of it makes known to the adverse party sufficiently in advance of the trial or hearing to provide the adverse party with a fair opportunity to prepare to meet it, the proponent's intention to offer the statement and the particulars of it, including the name and address of the declarant.

The purpose of FRE 807 is to allow evidence to be admitted when it is not specifically covered by some other exception to the hearsay rule, but is considered trustworthy. According to the

author of "Comptech Article", "[t]his guide may have inaccuracies, use at your own risk" (*see* "The CTDP Windows 2000 Tutorial Version 0.6.1 Oct. 28, 2001" (http://www.comptechdoc.org/os/windows/win2k/index.html) ("Introduction")); a copy of "Introduction" is attached hereto. As the author of "Comptech Article" has acknowledged the potential inaccuracy of the article, it would seem that "Comptech Article" is not sufficiently trustworthy to be admissible under FRE 807.

The Applicant recognizes that the Examiner might be attempting to argue that the Examiner's rejection is based not on the reference itself, but rather as "a teaching regarding the [Microsoft] Windows 2000" product as of its release date. If that is the case, then the rejection should not be centered around "Comptech Article", but rather on the Microsoft Windows 2000 product. But this does not relieve the Examiner's burden of establishing what was known before the filing date of the patent application; the Examiner has failed to meet this burden in this case. "Comptech Article" is a statement by its author that its author thinks Microsoft Windows 2000 included such authentication features at some unidentified date before October 28, 2001. "Comptech Article" cannot be read more broadly than this interpretation without becoming hearsay evidence.

The Applicant can only respond to the rejection the Examiner has made, and the Examiner has rejected the claims over "Comptech Article", not over Microsoft Windows 2000. But even if the Examiner is relying indirectly on "Comptech Article" to prove what was in Microsoft Windows 2000, the burden still lies with the Examiner to show that the claimed subject matter was published, known, or used by others before the filing date of the patent application: that is the reason behind the language in 35 U.S.C. §§ 102-103. To use "Comptech Article" in the manner the Examiner is proposing is to offer the reference "for the truth of the matter asserted", which is inadmissible hearsay.

- Assuming arguendo that "Comptech Article" is proper prior art, are the pending claims rendered obvious by "Comptech Article"?

 The Examiner has yet to properly reject claim 47

 First, the Applicant notes that the Examiner indicates that in the Office Action dated September 21, 2006, claims 1-47 are rejected as obvious over "Comptech Article", but provides no specificity as to why any of the claims are rejected. Claim 47 was added in the response to

the Office Action dated June 9, 2006, and therefore has never before been examined. Accordingly, the Examiner has failed to meet his burden of presenting a *prima facie* case of obviousness in rejecting claim 47.

The Examiner has improperly requested the Applicant to perform a search

Given that the Examiner continues to assert that "Comptech Article" is proper prior art in rejecting the claims and given the Examiner's remarks that the requested affidavit would make the claims allowable (see above), the Examiner has essentially challenged the Applicant to search for evidence that proves "Comptech Article" is not proper prior art. As argued above, this is an attempt by the Examiner to shift the burden of examination onto the Applicant and is inappropriate. Nevertheless, the Applicant's undersigned patent attorney has conducted a search in an attempt to determine exactly what Microsoft Windows 2000 offered in terms of authentication as of its initial release. On the premise that if anyone had published anything about authentication in Microsoft Windows 2000 before the filing date of this patent application it would have been Microsoft Corporation, the Applicant searched the knowledge base of the website of Microsoft Corporation for documents relating to authentication in Microsoft Windows 2000. The Applicant's search turned up one publication by Microsoft: "Basic Overview of Kerberos User Authentication Protocol in Windows 2000" (http://support.microsoft.com/?kbid=217098) ("Kerberos"). A copy was submitted with the Response to the Office Action June 9, 2006; another copy is attached hereto. This reference is not proper prior art any more than "Comptech Article" is proper prior art: no date of publication for "Kerberos" is provided, but "Kerberos" was last "reviewed" on November 21, 2003, and has a copyright date of 2006. "Kerberos" provides more detail about how Microsoft Windows 2000 performs authentication, and shows that some of the Examiner's interpretations of "Comptech Article" are erroneous, as discussed below. Thus, even assuming the Examiner's attempt to shift the burden of examination onto the Applicant was appropriate, the Applicant's search did not turn up any references that support the Examiner's rejection.

The Examiner's omnibus rejection of claims 4-18 and 23-46 is inappropriate

First, the Applicant notes that the Examiner only provides a specific rejection of claims 1-3 and 19-22. The Examiner has issued a summary rejection of claims 4-18 and 23-46, stating

that "such particular features are well known in the art for the purposes of handling information across computers" (*see* Office Action dated April 21, 2005, page 5). And even though the Examiner provides specific rejections of claims 2-3 and 20-22, the Examiner also rejects these claims as reciting features that the Examiner states were "known in the art". The Applicant respectfully disagrees. The Applicant asserts that these claims individually include features that are novel and non-obvious.

For example, claims 38-42 all recite a federation access policy. Notwithstanding the Examiner's statement "it was well known in the art to have a 'federated' situation among multiple computers that are networked and controlled with domain controllers, especially in domain controller that have group policy information which is replicated to all domain controllers" (*see* Office Action dated April 21, 2005, page 3), the Applicant respectfully asserts that a federation access policy was not known in the art at the time of invention. In particular, the Applicant asserts that a federation access policy used when two computers were in different domains was not known in the art. The Applicant points out that, for example, claim 1 recites a "cross-domain authentication apparatus", and "a first computer on a first domain and a second computer on a second domain". In other words, the domains in the claimed invention are different. This point is emphasized in new claim 47. The Examiner insists that it was known to have replicated domain information; but if the domains in the claimed invention are different, then the Examiner's assertion that a "'federated' situation" was well known is off point: the Examiner needs to show that it was known in the art to have a "'federated' situation" with different, non-replicated domains, as claimed.

While the Applicant has discussed only claims 38-42 and 47 in the above paragraph, the Applicant believes the other dependent claims also recite features that are patentable in their own right. The Applicant reserves the right to argue the independent patentability of claims 2-18 and 20-47, once the Examiner has supported his assertion that the features of these claims were "known in the art".

The Applicant also points the Examiner to M.P.E.P. § 707.07(d), which instructs the Examiner to provide specific rejections of the individual claims. M.P.E.P. § 707.07(d) states that "omnibus rejection of the claim 'on the references and for the reasons of record' is stereotyped and usually not informative and should therefore be avoided. This is especially true where certain claims have been rejected on one ground and other claims on another ground. A plurality

of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group." Thus, the M.P.E.P. instructs the Examiner to provide a specific rejection of the claims over the art. If the Examiner's assertion that "such particular features are well known in the art", then the Examiner should be able to provide one or more references that show that the features were "well known in the art"; the Examiner's cursory rejection of the claims is inappropriate.

"Comptech Article" does not teach a shared secret as claimed

Further problems exist within the Examiner's reasoning, even ignoring all of the other problems with "Comptech Article" availability as a reference under 35 U.S.C. § 102. The Examiner asserts that the password used in a domain logon is a "shared secret". The Applicant disagrees. The shared secret of the invention is a secret known in advance to each of the computers (*see* Specification, page 3, lines 3-4). But in a domain logon, the password is not known to the local computer until provided by the user. (If the password were known to the local computer, then the logon would be a local logon, and not a domain logon.) Therefore, the password cannot be a secret that is known in advance by each computer.

Another reason the password in "Comptech Article" cannot be the shared secret is that the password "is sent to the [Microsoft] Windows 2000 domain controller with an authentication request" (*see* "Comptech Article", "Process of Logging On", ¶ 2). The mere fact that the password is being sent to the domain controller establishes that the password is not a shared secret. Consider the situation where an unauthorized third party is attempting to access resources. Assuming the third party does not know the correct password, he would have to provide an incorrect password. But if the domain controller and the local computer "know" different passwords, the secret is clearly not shared.

It is also worth noting that step 325 of FIG. 3B, wherein the mediator performs the authentication, does not mention the shared secret. Instead, the shared secret is mentioned in step 340, wherein the random challenge nonce is encrypted using the shared secret. This shows that the user's password, which is used for user authentication, is different from the shared secret. If the password and the shared secret were meant to be the same element, the specification would have said so.

It could happen that the shared secret happens to be identical to the user's password. But if this situation arises, it is only by remote coincidence. As described in the specification, the user also has to provide his password to authenticate himself (if the local machine has not stored the authentication in advance).

In response to this argument, the Examiner states that "[a] shared secret is a secret that is shared. A password can be a secret. How can a password not be a secret?" (*see* Office Action dated April 21, 2005, page 2). The Applicant readily agrees that a password can be a secret. But the Examiner has overlooked, among other things, the significance of the word "shared": the fact that something is "secret" does not automatically mean that the secret is "shared".

It would appear that the Examiner is relying on the language in "Comptech Article" that "the name and password are checked against the local database" (*see* "Comptech Article", page 1). The Examiner's reasoning would appear to be as follows: "A password is a secret. The database knows the password, as (intuitively) does the user, so the password is shared. Therefore, the password is a secret shared, which meets the language of the claim."

The problem with this line of reasoning is that the Examiner overlooks the fact that the name and password are checked against the local database "[i]f the logon is local" (*see Id.*). A "local login" is where the user is logging into the local machine only; in this situation, there is no logon to the domain. That this situation excludes the possibility of a logon to a domain can be seen not only from the use of the term "local", but also from the next sentence in "Comptech Article", which begins "[i]f the logon is a domain logon . . ." (*see Id.*). The author of "Comptech Article" is contrasting the situation where the logon is to the local machine only against the situation where the logon is to a domain. If the logon is local, it is not a domain logon.

Having established that the logon in question in the first sentence of ¶ 2 of "Process of Logging On" in "Comptech Article" is a local logon, it should now be clear that the password cannot be a "secret shared" as claimed. Claim 1 recites "a secret shared between the first and second computers". In the local logon situation, the password is known only by the user and the local computer. Since the user is neither the "first computer" nor the "second computer", the password is not "a secret shared between the first and second computers". Thus, in the situation where the logon is local, a password is not a "secret shared" as claimed, and claims 1 and 27, both of which recite a "secret shared", are neither anticipated nor made obvious by "Comptech Article".

Actually, this whole line of reasoning suffers from another flaw: there is nothing that guarantees that the local computer stores the password in any accessible form. For security reasons, it is far more likely that the local computer stores a version of the password that has been passed through a one-way function. (A one-way function, as discussed below, is a function which generally cannot be reversed: given a particular output, it is difficult, if not impossible, to determine an input that the one-way function would convert to the particular output.) When the user provides the password, the computer immediately passes the received password through the same one-way function and compares that value with the value stored locally. If the local computer stores a hashed version of the password, then the local computer does not know the password, and so the password (the secret) is not "shared" at all.

There is a possibility that the Examiner was arguing that the password was a shared secret in the situation where the logon is a domain logon. In the domain logon situation, there are two computers. But in this situation, the two computers do not share the password. This can be seen from the fact that ¶¶ 3-4 of "Process of Logging On" in "Comptech Article" does not mention comparing the password received from the user with a database. Instead, the password and user name are "encrypted into a key" (*see Id.*).

The Examiner might argue that "encryption" suggests that the user name and password can be decrypted. The Applicant respectfully points out that this is not specifically stated anywhere in "Comptech Article"; the Examiner would therefore be drawing an unsupported inference. Further, the Applicant asserts that this decryption not only does not happen, but in fact cannot occur. The explanation why is below.

First, the Applicant points the Examiner to the first sentence of "Introduction", which is the introduction to the electronic document that includes "Comptech Article". According to the first sentence of "Introduction", "[t]his guide may have inaccuracies, use at your own risk". The author of "Comptech Article" has explicitly acknowledged that nothing he or she says is guaranteed to be accurate. Thus, where there is reason to believe the author is incorrect, the Applicant believes the author's statements should not be trusted. Given how cursory an explanation of domain logon the author of "Comptech Article" provides, the Applicant suggests the author of "Comptech Article" is glossing over many important details.

The Applicant points the Examiner to "Kerberos", mentioned above. The Applicant again points out that "Kerberos" is not proper prior art any more than "Comptech Article" is

proper prior art. But as "Kerberos" is authored by Microsoft Corporation, the company that developed, manufactured, and sold Microsoft Windows 2000, the Applicant respectfully submits that there is no better person or corporate entity capable of describing how Microsoft Windows 2000 performs authentication than Microsoft Corporation, its developer. Therefore, Microsoft Corporation is a more reliable source as to how Microsoft Windows 2000 operates than the author of "Comptech Article". According to "Kerberos":

> b. The Kerberos client sends a message to the Key Distribution Server (KDC), of type KRB_AS_REQ (Kerberos Authentication Server Request). This message has two parts:
>
> - An identification of the user, A, and the service for which she is requesting credentials, the TGS (Ticket-Granting Service).
> - Pre-authentication data, intended to prove that A knows her password. This is simply an authenticator encrypted with A's master key. The master key is generated by running A's password through a OWF.
>
> c. The KDC, upon receipt of KRB_AS_REQ from A, looks up the user A in its database (the Active Directory), gets her master key, decrypts the pre-authentication data, and evaluates the time stamp inside. If the time stamp passes the test, the KDC can be assured that the pre-authentication data was encrypted with A's master key, and is not merely a captured replay.

(*see* "Kerberos", page 1)

Given what is described in step c. about looking up user A in the database, this lookup would be performed based on the identification of the user, in the first part of the message sent to the KDC. After all, a password does not identify a user (using a password to identify a user would require that no two users share the same password, and rejecting a password as a duplicate would reveal that some user is using that password, information that is better kept secret). So the identification data does not include the password. This conclusion is reinforced by the second part of the message indicating that the pre-authentication data is used to prove that A knows her password (that is, to verify A's identity).

But neither does the pre-authentication data include the password. Note that the pre-authentication data is "simply an authenticator encrypted with A's master key" (*see Id.*). Further, according to step c., the "authenticator" includes a time stamp (presumably, of when the user attempted to log on, to protect against an intruder providing a copy of an earlier logon attempt). Given that there is separate mention of the "authenticator", the "master key", and the "password", it seems reasonable to conclude that these three items are distinct.

So if the authenticator is not the password, is the master key the password? No, it is not, as the master key is described as "generated by running A's password through a OWF" (*see Id.*). This, however, begs the question: what is an "OWF"? After all, if an "OWF" is an encryption algorithm, then the password might be recoverable by "decrypting" the master key.

The Applicant suggests that the acronym "OWF" stands for "one-way function". This is consistent with other uses of the acronym OWF by Microsoft Corporation. For example, the Applicant has attached a copy of "List of Security Fixes in Windows 2000 Service Pack 3" (http://support.microsoft.com/kb/324953/en-us) ("Security Fixes"). No date of publication for "Security Fixes" is provided; "Security Fixes" was last "reviewed" on March 9, 2006 and with a copyright date of 2006, and is therefore not proper prior art any more than either "Comptech Article" or "Kerberos" is proper prior art. But "Security Fixes" is not being presented for its content: "Security Fixes" is being presented to show a use of the acronym "OWF" in the context of Microsoft Windows 2000, and the definition of the acronym "OWF".

Bullet point number 2 of "Security Fixes" reads "Set LAN Manager (LM) One-Way Function (OWF) Password Results in Access Denied Error" (*see* "Security Fixes", page 1). While neither "Kerberos" nor "Security Fixes" defines what is meant by a "one-way function", it is commonly understood that a one-way function is a function that is difficult to invert: that is, given a result of the one-way function, it is difficult to determine the input to the one-way function that produced that result. For example, "one-way function from FOLDOC" (http://foldoc.org/foldoc.cgi?query=one-way+function&action=Search) defines "one-way function" as a "function which is easy to compute but whose inverse is very difficult to compute. Such functions have important applications in cryptography, specifically in public-key cryptography" (*see* "one-way function from FOLDOC", page 1). Because one-way functions are difficult to invert, given a known result it is difficult to find any input data that would produce the result, even if more than one input might produce the same result (which is not guaranteed: in general, there is no way to know how many inputs might produce a particular output). Hash functions are excellent examples of one-way functions, in that the original data cannot be recovered from the result of the hash.

Returning to "Kerberos", the master key is thus the result of sending the user's password through the one-way function. Because a one-way function is "one-way", the original password cannot be recovered from the master key: that is, the master key cannot be "decrypted". (It is

worth noting that, as one-way functions are hard to invert, and it is essentially impossible to find an input that returns a given result, an interloper would not be able to provide a password that would hash to the master key.) Thus, even if the master key is stored in the clear (where anyone could read it: this is unlikely in Microsoft Windows 2000 because the master key is used for encryption and decryption), the master key does not provide any information about the user's password.

So the user's password is not part of the identification data or the pre-authentication data, and is not derivable from any of that data or the master key. What does that mean? First, it is worth noting that the only data stored by the KDC in its database is the master key (presumably indexed by the user's identification). But if the password cannot be derived from the master key, then the password is not known by the KDC. This means that at least one of the two computers involved in domain logon in Microsoft Windows 2000 does not know the password, which means the password is not a "shared" secret.

Thus, given that the KDC does not store the user's password (instead storing the master key, derived from the password using a one-way function), and that the "Kerberos" client does not store the password either, the password is not a "secret shared". The password is a secret, yes; but it is a secret even from the computers, and so cannot be "a secret shared between the first and second computers", as claimed.

As "Comptech Article" does not teach or suggest a shared secret, whether using a local logon or a domain logon, claims 1 and 19 are patentable under 35 U.S.C. § 103(a) over "Comptech Article". Claims 1 and 19 are therefore allowable, as are dependent claims 2-18 and 20-47.

"Comptech Article" does not teach cross-domain authentication as claimed

As stated in the preamble of claims 1 and 19, the invention is directed toward an apparatus and method for cross-domain authentication. As described in the specification, cross-domain authentication is used where "an identity in one domain can be authenticated to another domain in the federation without actually creating an identity in the latter" (*see* Specification, page 2, lines 28-30). "Comptech Article" on its face is limited to two situations: local logons and domain logons (*see* "Comptech Article", Process of Logging On, ¶ 2). Neither of these

situations can handle a cross-domain authentication, where the computers involved are in different domains.

Although the Applicant believes that the preamble sufficiently describes claims 1 and 19 to distinguish the claims over "Comptech Article", claims 1 and 19 were previously amended to explicitly identify the computers as being on different domains. The Applicant also asserts that, because "Comptech Article" is not proper prior art and the amendments merely clarify features already present in the claims, these amendments to claim 1 and 19 were not narrowing amendments.

As "Comptech Article" does not teach or suggest cross-domain authentication, claims 1 and 19 are patentable under 35 U.S.C. § 103(a) over "Comptech Article". Claims 1 and 19 are therefore allowable, as are dependent claims 2-18 and 20-47.

The Applicant initially presented the foregoing argument in response to the Office Action dated September 8, 2004. To date, the Examiner has not responded to this argument. M.P.E.P. § 707.07(f) states that "[w]here the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it". As the Examiner does not respond to the argument that "Comptech Article" does not teach or suggest cross-domain authentication, the Examiner's Office Actions have been incomplete.

"Comptech Article" does not teach a "federated access policy" as claimed

In the Office Action dated September 8, 2004, the Examiner stated that "it was well known in the art to have a 'federated' situation among multiple computers that are networked and controlled with domain controllers – especially in domain controllers that have group policy information which is replicated to all domain controllers, such as in Microsoft Windows 2000 SYSVOL that is noted at the last sentence of the "Comptech Article" reference – for the motivation of having easier control of a group of domain controllers" (*see* Office Action dated September 8, 2004, page 3).

The Applicant asserts that whether or not a "federated situation" was known in the art, the Examiner has misread the claims. The claims describe a "federation access policy", which is distinguishable from a network of domain controllers. According to the specification, a "federation access policy is used to specify rights authorization of local resources to any identity in the federated identity space" (*see* specification, page 13, lines 20-21; *see also, e.g.*,

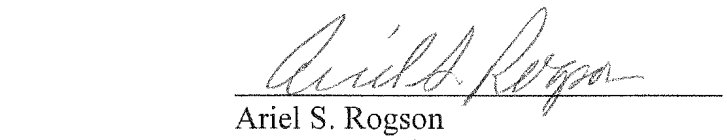
specification, page 2, lines 21-34 and page 5, line 18 through page 15, line 15). As a "federation access policy" specifies the rights authorization of local resources to an identity in the federated identity space" and a "federated situation" is a "federated network of computers", a "federated situation" has nothing to do with a "federation access policy", which the Applicant asserts is distinguishable. Thus, "Comptech Article" does not teach or suggest "a federation access policy identifying access permission on the first computer on the first domain for a user local to the second computer on the second domain over the network", as claimed.

As "Comptech Article" does not teach or suggest a federation access policy, claims 1 and 19 are patentable under 35 U.S.C. § 103(a) over "Comptech Article". Claims 1 and 19 are therefore allowable, as are dependent claims 2-18 and 20-47.

For the foregoing reasons, reconsideration and allowance of claims 1-47 of the application as amended is requested. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.



Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613
Customer No. 45842